REMARKS

This amendment is submitted in response to the final office action dated May 24, 2005. Reconsideration and allowance of the claims is requested. In this office action, all the claims were rejected as anticipated by or obvious over *Dorenbos* US 5,751,813. This rejection is respectfully traversed.

Dorenbos (5,751,813) column 3 lines 27-48 regarding the first-stage encrypted message is not for "privacy". Because it is encrypted by user's private key (as shown in Figure 2 and column 3 line 8-10), it is for authentication purpose. That is every body in the public can "decrypt" that first-stage message by user's public key (which by definition is publish in the public such every one can have access!) to verify whether this first-stage message is from the claimed user or not. Again, it is not for protecting the message from eavesdropping. The mechanism for protecting the eavesdropping in *Dorenbos* is the second-stage encrypting using server's public key; this is the single point of weakness in the system. If a hacker attacks the server successfully, he/she will be able to see all the message getting through the server using the server private key. Remember, the first-stage "encrypted" message can be decrypted by ANYBODY. Unlike the *Dorenbos* system, in this invention, if a hacker attacks the server successfully, he/she cannot decrypt the messages passing through the server at all.

Dorenbos column 3 lines 5 - column 4 line 10 is not a teaching of deriving share secret. The *Dorenbos* teaching is summarized below and then compared with the claimed invention.

Dorenbos teaching (system)

1) user "encrypt" (more precisely "sign") message (M) with his/her private key (ui) => Eui(M)

2) user encrypt Ui(M) with his/her ID and receipient ID1, ID2, .., IDn with server public key (sp) => Esp(Eui(M) + ID + ID1 + ID2 + .. + IDn)

3) server receive message Esp(Eui(M) + ID + ID1 + ID2 + .. + IDn) and decrypt it with server private key (si) => Dsi(Esp(Eui(M) + ID + ID1 + ID2 + .. + IDn))= Eui(M) + ID + ID1 + ID2 + .. + IDn

4) server uses table lookup to find ID1, ID2, .. , IDn's public keys u1p, u2p, .., unp on the server

5) server send out encrypted message Eu1p(Eui(M)+ID) to user1, Eu2p(Eui(M)+ID) to user 2, ..., Eunp(Eui(M)+ID) to usern.

Our invention

1) user requests receipients public keys (u1p, u2p, ..., unp) from server

2) user uses his/her own private key (ui) to derive share secret keys su1=ShareSecretFunction(ui,u1p), su2=ShareSecretFunction(ui,u2p), ... sun=ShareSecretFunction(ui,unp)

3) user encrypt the message (M) with share secret key (su1) => Esu1(M) and send Esu1(M) + ID to user1, similarly, Esu2(M)+ID to user2 ... Esun(M)+ID to usern.

4) server receives Esu1(M)+ID1, Esu2(M)+ID2,...,Esun(M)+IDn, it just passes them through to correspondent users, in this case user1, user2, ..., usern. No decryption and re-encryption is needed.

5) when user1 receives Esu1(M)+ID, he/she will requests sender (ID) public key (up) from server.

6) user1 will use his/her own private key ui1 to derive the share secret key us1=ShareSecretFunction(ui1,up). Mathematically we can prove that us1 will be equal to su1 (known in the skill of the art)

7) user1 will decrypt the receiving message using the us1 as Dus1(Esu1(M)) = M.

THE MAJOR DIFFERENCE of our invention is that if a hacker breaks in the server in our step 4, there is no way by using public keys in the server to decrypt Esu1(M), Esu2(M), ..., Esun(M). Because to decrypt these messages requires users' private keys information which are NOT stored in the server. The private key is stored in each individual user's PEAD. (On the contrary, public keys are stored in the server.)

On the contrary, if a hacker breaks in the server in step 3 of *Dorenbos* system, the hacker can decrypt Eui(M) by sender's (user's) public key which is stored in the SERVER! That is Dup(Eui(M))=M. Remember where do we get the user's public key (up) ---> it's from SERVER.

Notations: E is for encryption function, Ek means Encrypt with key k.
D is for decryption function, Dk means Decrypt with key k.

Symmetric key encryption background:

if a message M is encrypted with key k, then it can be decrypted by the same key k as shown in the following simple notation: Dk(Ek(M))=M.

Public key infrastructure background:

if a message M is encrypted with a public key (up), then it can be decrypted by its correspondent private key (ui): Dui(Eup(M))=M and vice versa Dup(Eui(M)).

In a public key infrastructure, the user needs to safe guard his/her own private key (ui), for example store a private key in his/her own PEAD and put the public key (up) to a public domain such as a server.

Encrypted in private key Eui(M) usually is called digital signature, which every one can validate it by request the public key from a server to decrypt the message Dup(Eui(M))=M. If decrypt successfully, it authenticates the user who claims who he/she is.

Encrypted in public key Eup(M) usually is for privacy. Because unless you have the user private key, NO Body else can decrypt the message except for the receiver who has the private key.

In view of these distinctions, reconsideration and allowance is respectfully requested.

Respectfully submitted,

John C. Carey
Registration No. 51,530
PATTERSON & SHERIDAN, L.L.P.
3040 Post Oak Blvd. Suite 1500
Houston, TX 77056
Telephone: (713) 623-4844
Facsimile: (713) 623-4846
Attorney for Applicant

PTO/SB/30 (04-05)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Request For Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COPY

Application Number	10/026,848
Filing Date	December 21, 2001
First Named Inventor	Ynjiun P. Wang
Art Unit	3621
Examiner Name	Mary Da Zhi Wang Cheung
Attorney Docket Number	ESX/007

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 C.F.R. 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
ii. ☐ Other _____

b. ☒ Enclosed

i. ☒ Amendment/Reply
ii ☐ Affidavit(s)/Declaration(s)
iii. ☐ Information Disclosure Statement (IDS)
iv. ☐ Other _____

2. Miscellaneous

a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. 1.103(c) for a period of _____months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. 1.17(i) required)

b. ☐ Other _____

3. Fees The RCE fee under 37 C.F.R. 1.17(e) is required by 37 C.F.R. 1.114 when the RCE is filed.

a. ☒ The Director is hereby authorized to charge the following fees, or credit any overpayments, to Deposit Account No. 20-0782/ESX/007/JAS . I have enclosed a duplicate copy of this sheet.

i. ☒ RCE fee required under 37 C.F.R. 1.17(e) $395.00
ii. ☒ Extension of time fee (37 C.F.R. 1.136 and 1.17) $510.00
iii. ☐ Other _____ Total: $905.00

b. ☐ Check in the amount of $ _____ enclosed

c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature		Date	November 23, 2005
Name (Print /Type)	John C. Carey	Registration No. (Attorney/Agent)	51,530

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print /Type)	John C. Carey	Date	November 23, 2005

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.